REMARKS

Claim Rejections

Claims 1-4, 8 and 16-19 stand rejected under 35 USC 103(a) as unpatentable over U.S. Patent Publication No. 2002/0071557 (Nguyen) in view of Federal Information Processing Standards Publication 186 (FIPS) and U.S. Patent Publication No. 2001/007127 (Staring).

Claims 5-7 and 20 stand rejected under 35 USC 103(a) as unpatentable over Nguyen in view of FIPS and Staring and further in view of U.S. Patent No. 5,885,158 (Torango et al.).

Claims 9-15 and 21-23 stand rejected under 35 U.S.C. 103(a) as unpatentable over Torango et al. in view of Nguyen, FIPS and Staring.

Specification Amendments

The specification has been amended to include the priority claim.

Claim Amendments

The claims have been amended to patentably distinguish over the cited references.

The Cited References

Nguyen discloses a gaming system in which gaming machines securely communicate with devices over a public network such as the Internet. (Abstract). The gaming system includes methods for providing gaming licenses, data acquisition and other gaming transactions. (¶0015). The system includes a method of sharing transaction data between a gaming machine and a remote server. The transaction data is encrypted and sent to the remote server. The transaction data includes accounting data, game usage data, game configuration data, software version data, etc. (¶0016). The system also provides for sending a game license request message from a gaming machine to a remote server. A game license reply message from the remote server includes a game license, updating the license data on the gaming machine. (¶0017). The system further provides for sending a gaming report request message from a gaming machine to a remote server, receiving a gaming report reply message from the remote server and when the gaming report reply message includes a gaming report, displaying the gaming report on a gaming machine. (¶0019). The remote server may also generate a reply message indicating that an original message from a gaming machine was received. The reply message may include the requested information. For instance, the remote server may request diagnostic data or a report of some type from the gaming machine. The data in the reply message may be encrypted. (¶0062).

FIPS discloses signature generation and verification techniques using a secure hash algorithum.

Staring discloses a communication system for the transfer of information from a source device to a sink device. The sink device includes a key resolver operative to determine which candidate session key corresponds to a source session key. (¶0014).

Torango et al. discloses a progressive gaming system. A win event can be automatically generated by a win of a progressive game event at a gaming terminal. (Col. 15, lines 41-51). A cluster controller determines whether the identity of a gaming terminal is valid. (Col. 16, lines 1-15).

Applicants' Claimed Invention Would Not Have Been Obvious

The cited references neither disclose not suggest Applicants' claimed methods, as set out in amended independent claims 1, 9, 16, and 21. Additionally, the cited references do not disclose the two-message procedure of claims 7, 14, and 19 or the single, signed message procedure of claims 8 and 15.

The independent claims as amended are not obvious in view of the cited references for at least the following reasons. By way of example, claim 1 is directed to a method of transmitting a command in a gaming network. Claim 1 recites generating a command originating at a master server or a slave server and digitally signing the command by performing a hashing function over at least a portion of a message that includes the command to produce a message digest. The message digest is passed through a digital signature algorithm to produce a digitally signed command including a session key that is changeable and associated with a current session index so that a receiving node can determine the session key used. An updated session index is periodically transmitted over the gaming network. The receiving node periodically compares the current session index to the updated session index, and the receiving node requests an updated session key when the current session index does not match the updated session index.

In one or more embodiments, as stated on page 10, lines 15-22 of Applicants' specification:

> All nodes are periodically informed of the current session key index through a plain text message the KDC broadcasts across the entire WAN every 10 seconds. When a node detects that the broadcast session key index identifying the current key is different from the index it has stored, it requests the new session key using a session key request procedure. Once it receives the new session key, the old session key is discarded. This procedure accommodates new

> devices, devices that have been offline when the period for changing session key passes (described below), and other situations in which a node does not have the current session key.

The cited references, considered alone or in combination, fail to disclose or suggest the above-noted features related to session keys of Applicants' claimed invention.

The Office Action states that the combination of FIPS and Nguyen fails to disclose or suggest "including a session key that is changeable and associated with an index so that a receiving node can determine the session key used." (Page 3, lines 15-17). Applicants agree with this assessment of FIPS and Nguyen. Further, since FIPS and Nguyen fail to disclose or suggest any feature related to session keys, FIPS and Nguyen also fail to disclose or suggest any "updated session index being periodically transmitted over the gaming network, the receiving node periodically comparing the current session index to the updated session index, and the receiving node requesting an updated session key when the current session index does not match the updated session index," as recited, for example, in amended claim 1.

The Office Action cites Staring as disclosing the claimed features related to session keys. (Page 3, lines 18-22). Staring does mention "a key generator" and "a key resolver." (¶ [0012]-[0014]). However, Staring fails to disclose or suggest any use of session keys as recited in the amended claims.

First, Staring fails to disclose or suggest any "session index being periodically transmitted over the gaming network," as recited, for example, in claim 1. Staring states that a sink device includes:

> [0012] a key generator for generating a plurality of candidate sink session key [sic] in a predetermined sequence of sink session keys Ksink.sub.i, where for each index i in the sequence the respective sink session key Ksink.sub.i corresponds to the respective source session key Ksource.sub.i;

As discussed in the above-quoted passage, each sink device in Staring includes a key generator. Further, each sink device must generate the keys to use for decryption, and the "index i" is used to ensure that the respective sink session key corresponds to the respective source session key. This allows the sink device to use a trial-and-error approach to determine the correct key for decryption by decrypting the same data using different ones of a plurality of keys. (¶ [0014]).

By contrast, amended claim 1 recites an "updated session index being periodically transmitted over the gaming network, the receiving node periodically comparing the current

session index to the updated session index, and the receiving node requesting an updated session key when the current session index does not match the updated session index." For example, as described in the above-quoted passage of Applicants' specification, in at least one embodiment, a receiving node is informed of the current session index by a message transmitted by the server every 10 seconds. Thus, a receiving node may determine whether the session key it is currently using is out of date by comparing its session index to the session index transmitted by the server. This allows the receiving node to identify the correct session key without requiring the receiving node to include a key generator or perform any trial-and-error decryption analysis to determine the session key. Therefore, the "index" mentioned in Staring (¶[[0012]-[0014]) is different than the session index as recited in claim 1.

Second, Staring fails to disclose or suggest "a session key that is changeable and associated with a session index so that a receiving node can determine the session key used," as recited in amended claim 1. Staring states that a sink device includes:

> [0014] a key resolver operative to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of [sic] each time a different one of the plurality of candidate sink session keys [sic] until a valid decryption result is found; and to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

As discussed in the above-quoted passage of Staring, each sink device includes a key resolver. Staring describes using a trial-and-error approach to determine the correct key. Specifically, the key resolver in Staring decrypts the same data using different ones of a plurality of candidate keys until the correct key is found.

By contrast, amended claim 1 recites "a session key that is changeable and associated with a session index so that a receiving node can determine the session key used." For example, in at least one embodiment, a receiving node can determine that a different session key is required by comparing a session index transmitted by the server with the session index of a session key in use by the receiving node. Then, the receiving node can request the correct session key from the server by using a session key request procedure. Thus, in one or more embodiments, the receiving node can determine and request the correct session key using the session index without the use of a key resolver and without the use of a trial-and-error approach. This may, for example, provide greater security and/or require less processing to perform

decryption than conventional methods. Staring fails to disclose or suggest a session index that allows the receiving node to determine the session key used.

Thus, the cited references, alone or in combination, fail to disclose or suggest any "session index being periodically transmitted over the gaming network" as well as any "updated session index being periodically transmitted over the gaming network, the receiving node periodically comparing the current session index to the updated session index, and the receiving node requesting an updated session key when the current session index does not match the updated session index," as recited in amended claim 1.

Therefore, Applicants' claimed invention would not have been obvious in view of Nguyen, FIPS, Staring or Torango et al.

Conclusion

In view of the foregoing, it is respectfully submitted that all the claims are now in condition for allowance. Accordingly, allowance of the claims at the earliest possible date is requested.

If prosecution of this application can be assisted by telephone, the Examiner is requested to call Applicants' undersigned attorney at (510) 663-1100.

If any fees are due in connection with the filing of this amendment (including any fees due for an extension of time), such fees may be charged to Deposit Account No. 504480 (Order No. IGT1P306X1).

Dated: March 18, 2009

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/William J. Egan, III/

William J. Egan, III
Reg. No. 28,411

P.O. Box 70250
Oakland, CA 94612-025030